

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
22 septembre 2005 (22.09.2005)

PCT

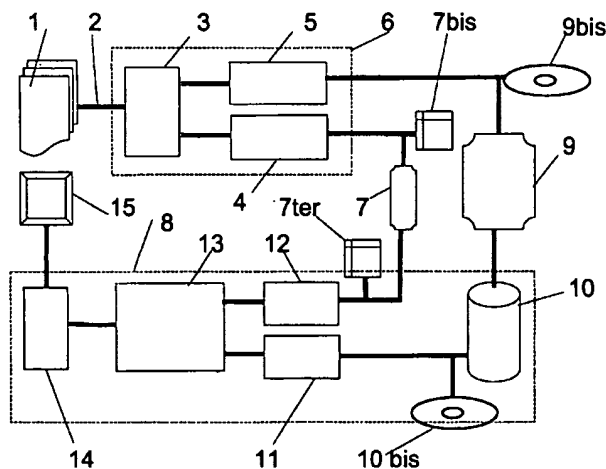
(10) Numéro de publication internationale
WO 2005/088902 A2

- (51) Classification internationale des brevets⁷ : H04L 9/34 (72) Inventeurs; et
(21) Numéro de la demande internationale : PCT/FR2005/000553 (75) Inventeurs/Déposants (pour US seulement) :
(22) Date de dépôt international : 8 mars 2005 (08.03.2005) LECOMTE, Daniel [FR/FR]; 157, rue de La Pompe,
(25) Langue de dépôt : français F-75116 Paris (FR). CAPOROSSI, Jérôme [FR/FR];
(26) Langue de publication : français 7, rue du 8 mai 1945, Bât. F, F-92340 Bourg-La-Reine
(30) Données relatives à la priorité : (FR). PARAYRE-MITZOVA, Daniela [FR/FR]; 88, rue
0450463 8 mars 2004 (08.03.2004) FR Philippe de Girard, Bât. B, Appt 132, F-75018 Paris (FR).
(71) Déposant (pour tous les États désignés sauf US) : MEDI- (81) États désignés (sauf indication contraire, pour tout titre de
ALIVE [FR/FR]; 111, avenue Victor Hugo, F-75116 Paris protection nationale disponible) : AE, AG, AL, AM, AT,
(FR). AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,
KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR THE SECURE DISTRIBUTION OF COMPRESSED DIGITAL TEXTS

(54) Titre : PROCÉDE ET SYSTEME DE DISTRIBUTION SECURISEE DE TEXTES NUMERIQUES COMPRESSES



(57) Abstract: The invention relates to a method for the secure distribution of compressed digital texts comprising blocks of binary data and resulting from transformations applied to an original text. The inventive method comprises two steps, namely: a preparatory step consisting in modifying at least one binary datum in one of the aforementioned blocks using at least one substitution operation involving the extraction of said datum from a block and the replacement thereof with a decoy; and a step consisting in transmitting (i) a modified compressed digital text (5) that conforms to the format of the original text, comprising blocks that were modified during the preparatory step, and, over a separate channel from the modified compressed text (5), (ii) a piece of complementary digital information (4) which can be used to restore the original compressed digital text (1) on the destination equipment from the modified compressed digital text (5) and said complementary information (4). The invention also relates to a system which is used to implement said method.

(57) Abrégé : La présente invention se rapporte à un procédé pour la distribution sécurisée de textes numériques compressés formés de blocs de données binaires, issus de transformations appliquées à un texte original, et comporte deux étapes : une étape préparatoire consistant à modifier au moins une donnée binaire dans un desdits blocs selon au moins une opération

[Suite sur la page suivante]

WO 2005/088902 A2



MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

de substitution consistant en l'extraction au sein d'un bloc de cette donnée binaire et son remplacement par un leurre, et une étape de transmission d'un texte numérique compressé modifié (5) conforme au format du texte original, constitué par des blocs modifiés au cours de l'étape préparatoire et par une voie séparée dudit texte numérique compressé modifié (5), d'une information complémentaire (4) numérique permettant de reconstituer le texte numérique compressé original (1), sur l'équipement destinataire, à partir dudit texte numérique compressé modifié (5) et de ladite information complémentaire (4). La présente invention concerne également un système pour la mise en oeuvre dudit procédé.